Elaborado por: William Ricardo Mateus Burbano.	Validado por: Cristian Alexander Alvarez	Aprobado por:
Fecha de elaboración: noviembre de 2018	Fecha actualización: 2020	Próxima actualización: Dos años a partir de la fecha

1. POLITICAS DE SEGURIDAD DE LA INFORMACION

Proteger los recursos de información de la ESE SANTIAGO DE TUNJA y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2. OBJETIVO

Implementar un plan de contingencia que garantice el adecuado funcionamiento del sistema de información en la ESE Santiago de Tunja, permitiendo garantizar la continuidad de las operaciones del sistema de información, definiendo acciones y procedimientos a ejecutar en caso de fallas.

3. OBJETIVOS ESPECIFICOS.

a. Reanudar con la mayor brevedad las funciones de la empresa, en pro de minimizar el impacto, para proteger el personal, minimizar el daño a operaciones, y equipo de procesamiento de datos (servidor), así como reducir la magnitud de la interrupción del servicio.

b. Evaluar los riesgos como los costos, cuando se presenta una interrupción del funcionamiento de la empresa, para invertir solo los recursos necesarios.

c. Optimizar los esfuerzos y recursos para atender cualquier contingencia de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes y durante la emergencia.

d. Proteger los datos generados por el sistema de información, mediante copias de seguridad y protección de la información.

4. ALCANCE

Garantizar el funcionamiento del sistema de información de la Empresa.

5. RESPONSABLE O DUEÑO DEL PROCESO

Líder Sistemas.

6. CAMBIOS EFECTUADOS

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
0	Procedimiento emitido en Versión 0 para prueba.	12-07-2012
1	Actualización del protocolo con inclusión de software Enterprise	06-12-2018

7. REFERENTE TEÓRICO Y DEFINICIONES

AMENAZA: Cualquier cosa que pueda interferir con el funcionamiento adecuado de un computador, a causar la difusión no autorizada de información contenida en un computador.

ANALISIS DE RIESGO: proceso sistemático para estimar la magnitud de los riesgos.

ARCHIVO: Es un elemento de información conformado por un conjunto de registros. Es decir que estos registros a su vez están compuestos por una serie de caracteres o bytes

ATAQUE: Acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información contenida en un computador.

ATAQUE ACTIVO: acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de un computador, o hace que se difunda de forma no autorizada información confiada a un computador personal. Ej, borrado intencional de archivos.

ATAQUE PASIVO: Intento de obtener información o recursos de un computador sin interferir con su funcionamiento, como espionaje electrónico, telefónico, o la interrupción de una red.

BASE DE DATOS: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Las bases de datos tradicionales se organizan por campos, registros y archivos. Un campo es una pieza única de información; un registro es un sistema completo de campos; y un archivo es una colección de registros. Por ejemplo, una guía de teléfono es análoga a un archivo. Contiene una lista de registros, cada uno de los cuales consiste en tres campos: nombre, dirección, y número de teléfono

CONFIABILIDAD: Propiedad de tener comportamiento y resultados previos consistentes.

CONFIDENCIALIDAD: Propiedad que determina que la información no este ni se divulgue a individuos, entidades o procesos no autorizados

CONTROLES BASICOS: Conjunto mínimo de salvaguardas establecidas para un sistema u organización.

COPIA DE SEGURIDAD: es el almacenamiento de las bases de datos y/o archivos residentes en los servidores y equipos propiedad de la Empresa, en un dispositivo de almacenamiento que además de garantizar su integridad y oportunidad, para realizar procesos de recuperación de información en los casos de siniestralidad, son un mecanismo de análisis histórico de operaciones.

DESASTRE: Se puede considerar como un desastre la interrupción prolongada de los recursos informáticos y de comunicación de una empresa, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

DVD: Es un dispositivo de almacenamiento óptico cuyo estándar surgió en 1995. Sus siglas corresponden con *Digital Versatile Disc*[1] en inglés (*disco versátil digital*). Un dispositivo de almacenamiento masivo de datos cuyo aspecto es idéntico al de un disco compacto, aunque contiene hasta 15 veces más información y puede transmitirla a la computadora unas 20 veces más rápido que un CD-ROM.

EVALUACION DEL RIESGO: proceso de combinar identificación, análisis y evaluación del riesgo.

GESTION DEL RIESGO: Proceso total de identificación, control y eliminación o minimización de eventos inciertos que pueden afectar los recursos de los sistemas de TIC.

IMPACTO: resultado de un incidente de seguridad de la información.

INCIDENTE DE SEGURIDAD DE LA INFORMACION: Evento inesperado o no deseado que puede comprometer las actividades de la empresa o la seguridad de la información.

INTEGRIDAD: Los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programa, del sistema, hardware o errores humanos.

NO REPUDIO: Capacidad para probar que una acción o un evento ha tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PLAN: es una intención o un proyecto. Se trata de un modelo sistemático que se elabora antes de realizar una acción, con el objetivo de dirigirla y encauzarla. En este sentido, un plan también es un escrito que precisa los detalles necesarios para realizar una obra.

PLAN DE CONTIGENCIA: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

Esta clase de plan, garantiza la continuidad del funcionamiento de la empresa frente a cualquier eventualidad, ya sean materiales o personales.

Un plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad y operaciones de la empresa.

Un plan de contingencia es una estrategia planificada continuada por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminados a conseguir una restauración progresiva y ágil de los servicios de la empresa por una paralización total o parcial de la capacidad operativa de la empresa.

PLAN DE CONTINGENCIA EN SISTEMAS: consiste en los pasos que se debe seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema

PRIVACIDAD: Derecho que tienen los individuos y organizaciones para determinar ellos mismos, a quien, cuando y que información referente a ellos serán difundidas y trasmitidas por otros.

RECUPERACION: Capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, habiendo reemplazado o recuperado el máximo posible de los recursos e información.

La recuperación de la información se basa en el uso de una política de copias de seguridad adecuada.

RESTAURACION: acción de tomar una copia de seguridad y emprender las actividades encaminadas a restablecer un archivo o documento con corte a una fecha determinada

REGISTRO: Es el conjunto de información referida a una misma persona u objeto. Un registro vendría a ser algo así como una ficha.

RIESGO: Potencial de que una amenaza determinada aproveche las vulnerabilidades de un activo o grupo de activos y produzca daño a la empresa. Se mide en términos de la combinación de la probabilidad

SALVAGUARDA: práctica, procedimiento o mecanismo para tratar los riesgos.

SEGURIDAD DE LA INFORMACION: todos los aspectos relacionados con la definición, el logro y el mantenimiento de confidencialidad, integridad, disponibilidad, no repudio, trazabilidad, autenticidad y confiabilidad de la información o de los servicios procesados de información.

SERVIDOR: es un computador cuyo propósito es proveer datos o servicios de modo que otros computadores los puedan utilizar y administrar las bases de datos en las que se almacena la información de los procesos que cuentan con aplicativos residentes en el.

TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de controles para modificar el riesgo.

VULNERABILIDAD: debilidad de un activo o grupo de activos que puede ser aprovechada por una o mas amenazas.

8. PLAN DE CONTINGENCIA SISTEMAS DE INFORMACION

8.1 DIAGNOSTICO

8.1.1 ORGANIZACIÓN ESTRUCTURAL Y FUNCIONAL

Ver anexo 1

8.1.2 SERVICIOS

La ESE Santiago de Tunja, presta servicios de salud de primer nivel de atención, ambulatorio, cuenta con nueve puestos de salud distribuidos en la ciudad.

8.1.3. INVENTARIO INFORMATICO

El inventario informático reposa en almacén y en las carpetas de las hojas de vida de los equipos de computo

RELACION DE LOS SISTEMAS DE INFOMACION.

NOMBRE DEL SISTEMA	AREA QUE GERERA LA INFORMACION	QUIENES USAN LA INFORMACION	VOLUMEN DE LA INFORMACION	VOLUMEN DE LAS TRANSACCIONES
CNT PACIENTES	Consultorio médicos, odontológicos, facturación	Líderes de medicina, odontología, salud publica	Alto	Diaria
INVENTARIOS (FARMACIA)	Consultorios médicos y odontológicos, farmacia	Líder de medicina, farmacia	Alto	Diaria
LABORATORIO CLINICO	Consultorios médicos, bacterióloga	Médicos, bacterióloga	Alto	Diaria
FACTURACION	Caja, puestos de salud	Facturación	Alto	Diaria
CUENTAS POR PAGAR	Tesorería	Gerencia, tesorería, contabilidad, presupuesto.	Medio	Diaria
CUENTAS POR COBRAR	Tesorería	Gerencia, auditoria, cartera, contabilidad	Medio	Mensual

CONTABILIDAD	Contabilidad	Gerencia, contabilidad.	Medio	Diaria
ACTIVOS FIJOS	Almacén	Almacén, contabilidad	Bajo	Mensual
NOMINA	Subgerencia	Gerencia, subgerencia	Bajo	Mensual
PRESUPUESTO	Presupuesto	Gerencia, tesorería, contabilidad, presupuesto	Medio	Diaria

8.2. IDENTIFICACIÓN DE LOS FACTORES DE RIESGOS:

RIESGOS DE SOFTWARE	RIESGOS DE HARDWARE
Virus	Interrupción suministro de energía
Hackers	Errores de hardware
Errores en el software	Interrupción del servicio de red
Interrupción suministro de internet	Daño en servidor

RIESGOS HUMANOS

DELIBERADOS	ACCIDENTALES
Escuchas no autorizadas	Errores y omisiones
Modificaciones de la información	Eliminación de archivos
Piratería en sistemas de información	Accidentes físicos
Robos	

8.2.1. ANALISIS Y EVALUACION DE RIESGOS

SERVICIOS AFECTADOS	PROCESOS AFECTADOS	PROCESOS CRITICOS DEL SERVICIO
Consulta medica	Historia clínica	Historia clínica
Consulta odontológica	Historia clínica	Historia clínica
Facturación	Cargo de servicios, citas medicas, agendas	Cargo de servicios
Cartera	Ingreso de facturación, reportes de cartera	Ingreso de facturación
Contabilidad		
Tesorería	Generación de giros	Generación de giros
Presupuesto	Generación de certificados de disponibilidad, registros, obligaciones, giros	Generación de certificados de disponibilidad, registros, obligaciones, giros

Farmacia	Ingreso medicamentos al sistema	Ingreso medicamentos al sistema

8.3 ESTRATEGIAS GENERALES.

8.3.1. Copias de seguridad de toda la información en medios magnéticos, CD, DVD. Estas serán de solo la información, de las aplicaciones no.

8.3.2. Tener antivirus recientes y actualizados.

8.3.3. El acceso al centro de computo debe estar restringido al personal autorizado. El personal de la institución deberá tener carnet de identificación en lugar siempre visible.

8.3.4. El acceso a los sistemas multiusuarios (red) y a los archivos contenidos en dichos sistemas deben estar controlados mediante la verificación de usuarios (manejos de perfiles para el ingreso, usuarios y contraseñas)

8.3.5. Políticas para la creación de contraseñas y cambio periódico de las mismas.

8.3.6. La seguridad de las unidades de CD, puestos UBS, deben ser controladas, para que de esta manera se asegure la información contra robos y acceso de virus informáticos.

8.3.7. Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

8.3.8. Todos los medios magnéticos deben estar identificados, que definan su contenido y su nivel de seguridad.

8.3.9. El control de los medios magnéticos debe ser llevado mediante inventario periódico.

8.3.10. Toda impresión que contenga información confidencial, debe ser destruida.

8.3.11. Etiquetar los equipos de cómputo de acuerdo a la importancia de su contenido: color rojo a los servidores, amarillo a los computadores con información importante, verde a los demás computadores.

OBTENCION Y ALMACENAMIENTO DE LOS RESPALDOS DE INFORMACION (COPIAS DE SEGURIDAD)

Establecer un procedimiento de copias de seguridad de todo el software necesario para asegurar el correcto funcionamiento de la organización.

- Copia de seguridad de cada uno de los sistemas operativos
- Copia de seguridad de cada uno de los aplicativos.
- Copia de la base de datos y todo archivo necesario para la correcta ejecución de los aplicativos.

Para la realización de las copias de seguridad se debe tener en cuenta:

- Periodicidad del tipo de copia.
- Uso de un formulario para el registro y control de las copias de seguridad.
- Almacenamiento de las copias de seguridad en condiciones ambientales optimas dependiendo del medio magnético empleado.
- Almacenamiento de las copias de seguridad en locales diferentes donde se encuentra la información primaria
- Pruebas periódicas de las copias de seguridad, verificando su funcionalidad.

Cuando ocurra una contingencia, y si se tiene el conocimiento del motivo que lo originó y el daño producido, esto permitirá en el menor tiempo posible la recuperación del proceso perdido.

9. PLAN DE CONTINGENCIA SISTEMAS DE INFORMACION

9.2. VIRUS

ANTES	DURANTE	DESPUES
Actualmente la empresa NO cuenta con un software antivirus corporativo licenciados el cual se tiene instalado en todos los equipos de cómputo de la institución. Para evitar el ingreso de virus a los equipos de cómputo, es necesario bloquear los puertos de ingreso de la información como son unidades de CD, DVD o USB; y hacer escaneo de los dispositivos antes de abrirlos. Realización de copias de seguridad de los equipos	Apagado del equipo Reporte inmediato al área de sistemas del problema. En el momento que se compruebe que un equipo contiene virus que puede dañar la información contenida en este o contaminar otros equipos, el área de sistemas procederá a recuperación de datos si hay lugar, limpieza y formateo según sea el caso.	Vacunación periódica de los equipos, escaneo de los dispositivos externos que se introduzcan en los equipos, antes de abrir cualquier tipo de información. Recomendaciones generales.

9.3. HACKERS.

ANTES	DURANTE	DESPUES
Uso de perfiles de usuarios, asignación de contraseñas para el ingreso a las aplicaciones, la red y el uso de los recursos. Restricciones de acceso para ingreso a la información.	Bloqueo usuario. Detención de la base de datos	Revisión de la base de datos para verificar que no haya ataques y puesta en marcha de la misma. Reasignar usuarios y contraseñas, entrega a los usuarios del sistema

9.4. ERRORES EN EL SOFTWARE

ANTES	DURANTE	DESPUES
En el momento de la realización de actualizaciones en las aplicaciones con que cuenta la ESE Santiago de Tunja, se hace necesario la realización de pruebas de funcionamiento en una base de datos diferente a la de producción, esto con el fin de evitar inconvenientes en el momento la puesta en marcha de la aplicación.	Reporte inmediato al área de sistemas del problema. No ingreso de información al sistema, realización de registros de forma manual. Reemplazo de equipo de cómputo mientras se hace el mantenimiento y arreglo del sistema.	Ingreso al sistema, diligenciamiento, registro y actualización de la información registrada en medio físico.

9.5. INTERRUPCIÓN EN EL CANAL DE DATOS.

ANTES	DURANTE	DESPUES
Verificación continua de la trasmisión de datos en los canales de información de la empresa	Reporte al área de sistemas del problema. Cuando de presenten interrupciones en el suministro de internet, se hace necesario que	Si trascurrido este tiempo se verifica que la información no ha sido ingresada en el sistema, se procederá a notificar al responsable y se procederá a la eliminación

	el profesional haga el registro del momento de la caída y proceda a la realización de la Historia Clínica en medio físico, la cual el profesional responsable tendrá un plazo de 5 días hábiles para el ingreso de la información al sistema.	de los cargos que se encuentren sin diligenciar.

9.6. INTERRUPCIÓN SUMINISTRO DE ENERGÍA.

ANTES	DURANTE	DESPUES
Suministro de UPS a los equipos de la empresa, por tal razón en el momento de haber cortes de energía, el funcionario tiene un plazo prudente (aprox 15 min) para guardar la información y apagar el equipo de cómputo mientras se restaura la energía. El centro de salud numero uno cuenta con planta eléctrica de encendido automático.	Reporte al área de sistemas del problema. En caja: registro de la información en medio físico. Medicina y odontología: realización de Historias en medio físico, para lo cual el profesional realizará el ingreso al sistema	En el momento de la restauración de la energía se procede al ingreso de la información. Si el inconveniente es el daño en las UPS, el área de sistemas procede al cambio de la misma

9.7 ERRORES DE HARDWARE

ANTES	DURANTE	DESPUES
Contar y ejecutar un programa de mantenimiento preventivo y correctivo a los equipos de cómputo de la empresa, impresoras, scanner.	Reporte al área de sistemas del problema. Reemplazo del equipo que se encuentra en mal funcionamiento mientras se realizan los cambios de las piezas defectuosas. Reemplazo total del equipo, cuando este no tenga arreglo.	Entrega del equipo arreglado o cambio del mismo según sea el caso.

9.8. INTERRUPCIÓN DEL SERVICIO DE RED

ANTES	DURANTE	DESPUES
Se establece que los equipos estén identificados con una dirección IP, la cual es única, la cual es conocida únicamente por el administrador. Se define que los usuarios no cuenten con permisos para instalar, desinstalar o modificar programas y configuración de cada uno de los equipos.	Reporte inmediato al área de sistemas del problema. Si no hay acceso a la red de datos de la empresa, el funcionario hace el reporte al área de sistemas. Verificación de la red de datos, realización de pruebas de conexión Registro de información en medio físico mientras hay la restauración del sistema	Por parte del área de sistemas: Cambio de cables de red, swich, puertos de red, reemplazo de equipo. Digitación e ingreso de la información al sistema.

9.9. DAÑO EL SERVIDOR.

ANTES	DURANTE	DESPUES
Restricción de acceso para ingreso al área de sistemas, solo puede ingresar el administrador del sistema. No permitir que personas que no han de utilizar el servidor estén cerca de él. Por la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local). Establecer un espacio seguro con un espacio que limite al acceso a personal no autorizado. Establecer un medio de control de entrada y salida de visitas al centro de cómputo El acceso a los sistemas compartidos por	Conocer al detalle el motivo que origino la falla y el daño producido. Diligenciamiento de la información en medio físico mientras se hace el restablecimiento del sistema. Restablecer en el menor tiempo posible el nivel de operación normal del procesamiento de la información.	Evaluación de la magnitud del daño. Restauración de copias de seguridad Montar la base de datos en un servidor alterno. Adquisición de servidor de acuerdo a la falla o problema que haya tenido.

múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados Políticas para la creación de los password y establecer periodicidad de cambios de los mismos. Ubicación y señalización de los elementos contra el siniestro (extinguidores)		

9.10. ERRORES HUMANOS

ANTES	DURANTE	DESPUES
Capacitación del personal en cuanto al manejo de los equipos, política y procesos del sistema de información. Supervisión periódica del desarrollo de los procesos establecidos por el sistema de información.	Reporte al área de sistemas del problema. Evaluación del impacto del evento ocurrido. Controlar el evento y las posibles consecuencias	Mediante la evaluación del evento establecer plan de mejoramiento, para evitar que se vuelva a presentar.

10. FORMATO REPORTE DE FALLAS.

EMPRESA SOCIAL DEL ESTADO SANTIAGO DE TUNJA
FORMATO REPORTE DE FALLAS (FO-ST-01)

	FECHA		HORA	
NOMBRE DE QUIEN REPORTA				
CENTRO DE ATENCION				
AREA				
TIPO DE FALLA				
DESCRIPCION DE LA FALLA:				
FORMA DE QUIEN REPORTA				

11. FLUJOGRAMA